Délits informatiques et preuve

Le défi de l'impossible ?

Speaker :
Marie BAREL,
juriste spécialisé
« TIC et Sécurité de l'information »

Objectifs 25’ chrono » !

1. Préalable nécessaire : la question de la loi applicable

En droit français …

- 2. Comment prouve-t-on devant un juge pénal ? : principes de l’administration de la preuve
  - Système de liberté de la preuve
  - Système de l’intime conviction
- 3. Que doit-on prouver ? : les difficultés de la preuve … informatique
  - Force probante des « preuves informatiques »
  - De l’intention et de l’imputabilité : quelle riposte face à la « *trojan defence* » ?

1. De la loi applicable ?

- Des délits « pluri-localisés » dont l'appréhension nécessite une coopération internationale, une volonté politique et des moyens adaptés

USA v. Zezev (2003) : « Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion »

USA v. Ivanov (2003) : « Russian Man Sentenced for Hacking into Computers in the United States » (2 years in prison + 3 years of supervised release) ;

USA v. Gorshkov (2002) : « Russian computer hacker sentenced to 3 years in prison » and ordered to pay 700.000 $ for the losses he caused. Pour arrêter les pirates, le FBI crée une start-up de sécurité informatique.

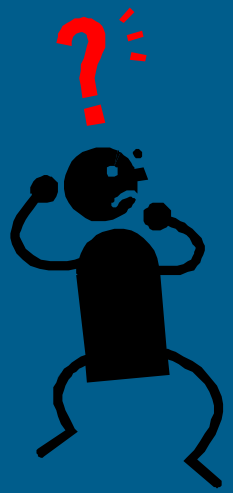
USA v. Ehud Tenenbaum (1998) : « Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers » (12 mois de mise à l'épreuve et 17.000 $ d'amende)

➥ **CCIPS :**
http://www.cybercrime.gov

De la loi applicable ?

- En matière de délits commis sur les réseaux (en particulier l'Internet), la loi est omniprésente plutôt que l'inverse : « *la particularité sans doute unique d'être soumis à toutes les lois de tous les Etats du monde* » (A. Cousin)

- Cependant, l'applicabilité de la loi ne présume pas :
  - des risques de distorsion entre les différentes législations
  - des difficultés pratiques notamment d'ordre procédural (ex. circuit de transmission des CRI)
  - de l'effectivité des décisions prises à l'encontre de personnes résidant hors de France



Solutions ?

- Harmonisation des textes répressifs et nouveaux moyens d'enquête
- Accords de coopération et d'entraide policière et judiciaire (ex. Europol, Eurojust)
- Accords en matière d'extradition

Instrument juridique international : Convention sur la cybercriminalité (EEV 2004)

De la loi applicable ? (2/4)

- **Enjeu de la détermination de la loi applicable : définit les REGLES DE PROCEDURE A SUIVRE, LE REGIME JURIDIQUE DE LA PREUVE, VOIRE L'EXISTENCE MÊME DE L'INFRACTION**
  - **Cas d'application de la loi pénale française pour des infractions commises à l'étranger (non exhaustif) :**
    - À l'encontre d'un complice en France (art. 113-5 CP)
    - Pour tous crimes et certains délits commis par un Français (art. 113-6 CP)

      CONDITION : **sous réserve de réciprocité d'incrimination**

Ex. : accès indu dans un système d'information

- Pays où l'infraction initiale (accès non autorisé à un système d'information) …**existe en tant que telle** :

  Afrique du Sud – Belgique – Chili – Corée – Danemark – France (323-1 al.1) – Finlande – Grèce – Irlande – Islande – Israël – Luxembourg – Malaisie – Malte – île Maurice – Nigeria (draft) – Nouvelle-Zélande – Philippines – Roumanie (draft) – Singapour – UK – Venezuela – la majorité des États des USA – …

- Pays où la même infraction existe **à condition que** :
  - les données ou le système accédés soient protégés par des mesures de sécurité (accès restreint) :

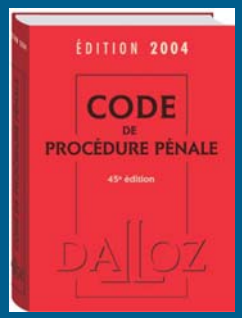
    Allemagne – Argentine – Australie – Croatie – Estonie – Hongrie – Italie – Japon – Mexique – Norvège – Pays-Bas – Pologne – Suisse – …
  - l'intrusion ait été suivie d'effet (copie, altération, suppression de données, … dommages) ou soit animé par un esprit de fraude :

    Bengladesh – Bulgarie – Chine – Espagne – Pérou – Ukraine – certains États des USA – …
  - moyennant plusieurs des conditions susvisées ou d'autres conditions :

    Canada – Lettonie – Portugal - République tchèque – Russie – Suède – …
- Pays où l'infraction **n'existe pas** : *Inde – …*

2. Comment prouver en droit pénal français ?

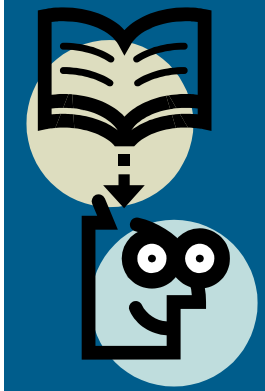
- La preuve au pénal
  - Principe de la présomption d'innocence : oblige le plaignant (Min.Public, parties civ.) à prouver la culpabilité, à détruire le doute qui profite à l'accusé.



  - Principe de liberté de la preuve : article 427 CPC, « *par tout mode de preuve* »
    - Faits juridiques / actes juridiques
    - Recevabilité en justice des « preuves informatiques » (ex. *logs, mails, documents électroniques, …*) : ne présume pas de leur valeur probante !

Comment prouver en droit pénal français ? (2/5)

- Limites au système de preuve libre : rejet des procédés de preuve illicites ou déloyaux
  - Condition première de la reconnaissance de la loyauté de la preuve, le respect des droits de la défense (ex. protection de la correspondance avec son avocat)
  - Sanctionne les abus dans la recherche de la preuve et les méthodes d'investigation : pratiques contraires à la dignité humaine (torture, traitements inhumains ou dégradants, respect de l'intégrité physique ou atteinte à la volonté: narco-interrogatoire, hypnose, …) ou à la dignité de la Justice (Cf. provocations policières)
  - La disqualification de la preuve peut être totale ou partielle, suivant 'l'ampleur de la déloyauté' (« preuve parfaite » ex. aveu, preuve par écrit, … ➲ valeur indiciaire)



Comment prouver en droit pénal français ? (3/5)

- Le **principe de loyauté et de légalité** dans l'administration de la preuve : **une application différenciée** selon la personne concernée (**personnes privées** / autorités publiques)

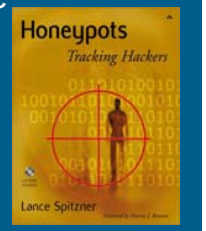
  - Affaire SOS Racisme / procédé de *testing* (discrimination raciale à l'entrée des discothèques et autres lieux de divertissement nocturnes) – Cass. Crim, 15 juin 1993 ; Voir aussi : Crim., 11 juin 2002 – http://www.courdecassation.fr/arrets

Attendu de principe : « *Attendu qu'aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale ; (…).* »

Commentaire de l'avocat général : « *(en droit français), la production de la preuve est libre , d'autant plus lorsqu'elle est rapportée par un particulier qui n'a pas, au contraire des policiers et des gendarmes, à respecter le code de procédure pénale* ».

Ex : les *honeypots* sont-ils légaux ? > lorsqu'ils sont mis en œuvre par une personne privée, les procédés de collecte de données activés dans le cadre de systèmes pot de miel ne peuvent être écartés « par principe ».

ATTENTION ! : effets de l'inobservation du principe de légalité à l'égard de l'auteur de l'acte illicite = risque de poursuite judiciaire.



Comment prouver en droit pénal français ? (4/5)

- « *Le juge décide d'après son intime conviction.* » (art. 427 CPC précité)
  - « *Libre appréciation* » de tous les éléments de preuve qui sont apportés devant le tribunal (y compris ex. en matière d'aveu : art. 428 CPC)
  - J. Pradel : équivalent exact du concept anglo-saxon « *beyond reasonable doubt* », signifie que l'on a atteint un « *haut degré de probabilité sans toutefois parvenir à une certitude* » (Lord Denning).

Comment prouver en droit français ? (5/5)

NO MATCH !

Nom du suspect : E.T.

Identifiant : 0000001

Empreinte :

- Résultats recherche :
  10^{-0} près

- Cause probable :
  origine extra-terrestre

- La preuve probabiliste***, un droit de citer ?

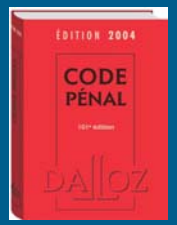
*** Définition : système dans lequel la force probante d'une preuve est mesurée par sa probabilité de fraude

Preuve juridiquement > , si probabilité fraude <

- La preuve statistique admise devant les tribunaux …
  - Identification par empreinte digitale : 10^{-4} près
  - Identification par empreinte génétique (ADN) : 10^{-9} près
- … mais sans lui accorder de force supérieure aux autres modes de preuves

  - ex. en matière d'écrit et de signature électronique dont la probabilité de fraude est inférieure à celle du document et de la signature manuscrite : le juge détermine « *le titre le plus vraisemblable, quel qu'en soit le support*. » (art. 1316-2 C.Civ.)

3. Que faut-il prouver ?



- Élément légal : '*nullum crimen, nulla poena sine lege*'

  Ex. de référence : constat d'une activité sur un système pot de miel
  > nécessité de qualifier l'infraction

  - 323-1 CP : accès (suivi d'un maintien) frauduleux dans un STAD

- Élément matériel : ex. un « accès »

  Deux acceptations :

  - sens actif : accès technique
  - sens passif : interception

- Élément moral ou psychologique : un acte volontaire, fait « *sans droit et en connaissance de cause* » (CA Paris, 5 avril 1994)

Difficulté 1 : valeur probante

- La fiabilité des preuves informatiques : une appréciation libre occasionnant des variations dans les décisions

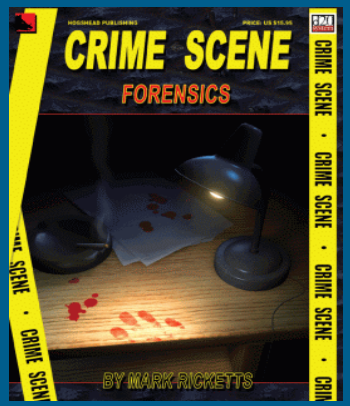
  Exemple :

  - Affaire *Crédicas*, 1989 (acceptation) : « *il n'est allégué aucun dérèglement du système informatique* (…) »
  - CA Paris, 12 décembre 1980 (rejet) : la preuve de l'absence de défaillance, une charge très lourde pour le demandeur !

- Conditions d'une preuve informatique « irréprochable » : état de l'art du *forensique*

  - Précautions techniques pour la capture, la conservation et l'analyse des données : ex. des *honeypots* (MISC 8)



  - ✓ Multiplication des sources : recoupements, reconstruction des séquences d'attaques favorisés, sauvegarde
  - ✓ Conservation non pas en local mais sur un système tiers de confiance : retour sur expérience (attaque contre une machine protégée), mise en évidence d'actions antiforensiques
  - ✓ Analyse *post mortem* à partir de données copiées (copie fidèle, bit à bit ; supports non réinscriptibles ou systèmes de confiance ; empreinte MD5 des sorties)
  - ✓ Tenue d'un « cahier d'opérations » (extraction, analyse) : chemin menant à la preuve, traçabilité/imputabilité

Difficulté 2 : intentionnalité

- « A l'insu de son plein gré » ou « *en pleine connaissance de cause* » (CA Paris, 5.04.1994) ? : quelques facteurs discriminants
  - Nombre de barrières techniques et robustesse des mesures de sécurité contournées : analogie du « double clic » et qualification du niveau de compétence requis/évalué
  - Action anti-forensique (Cf. Laurent Roger/CELAR, *Antiforensic* – SSTIC'05) et refus de collaborer : ce qu'on cache vaut bien ce qu'on trouve !

Légende : « J'ai l'impression d'avoir fait quelque chose d'interdit !?! »

Difficulté 3 : imputabilité (1/2)

- De l'art d'insuffler le doute au profit de l'accusé ! : le péril de la « *Trojan defense* » :

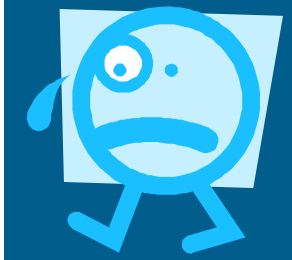
Source image : http://www.sophos.com/virusinfo/articles/caffrey.html

« Computer did it ! »

Jury trusts …

- Juillet 2003, *Regina v. Green* (UK) : accusation de pédopornographie - acquittement - témoignage d'un expert - présence de 11 Chevaux de Troie sur le PC de l'inculpé -
  Fait suite à une affaire similaire en avril 2003 pour des faits et des circonstances similaires (affaire *Regina v. Karl Schofield).*
- Octobre 2003, *Regina v. Caffrey* (UK) : accusé d'avoir lancé un déni de service distribué (DDOS) qui a fait « tomber » plusieurs systèmes informatiques du port de Houston (Texas) en septembre 2001.
  Éléments à charge :
  - ✓ Copie du **script** de l'attaque sur le disque dur
  - ✓ Script portant une **dédicace** à « Jessica » (prénom de sa petite amie) et une **signature** « Aaron »
  - ✓ **Témoignage de l'expert** : aucune preuve de la compromission de la machine ; aucune altération des fichiers de *logs*
  - ✓ Appartenance au groupe *Allied Haxor Elite* (objet : tests d'intrusion « à titre amical » et moyennant autorisation préalable) >>> atteste un **niveau compétence** suffisant pour écrire le script de l'attaque et l'exécuter.

Difficulté 3 : imputabilité (2/2)



- De l'art d'insuffler le doute au profit de l'accusé ! (suite)
  - Les avancées techniques en matière de traçabilité (*port scan, markers e.g.)* encore utiles ? : pas de contestation de l'origine de l'attaque
  - L'expertise technique comme support de la défense : l'attaque ou l'action litigieuse a pu être effectuée sans la connaissance ni la permission de l'utilisateur.
- Les tribunaux anglo-saxons plus « fragiles » devant la *trojan defense ?*
  - Particularité du système pénal anglo-saxon : la composante de jury
  - Difficulté de la preuve *négative* à charge du demandeur dans le système français (Cf. *supra*)
- Une réponse scientifique ? : modélisation proposée par Megan Carney et Marc Rogers pour définir les facteurs discriminants permettant au juge de conclure à l'innocence ou la culpabilité du prévenu (*Intl Journal of Evidence* – Spring 2004, vol. 2, issue 3).

Conclusion

Countdown

00 : 24 : 59

- CONTACT : marie.barel@legalis.net